Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) An unauthorized use prevention apparatus included in an information processing device, comprising:

a speech feature memory storing identifying speech feature data previously obtained from voice of an authorized user;

a password generator for generating a password which is a string of arbitrary characters;

a password notifying section for notifying a present user of the generated password;

a speech feature extractor for extracting speech feature data from voice of the present user to produce input speech feature data;

a speech feature comparator for comparing the input speech feature data to the identifying speech feature data to produce a speech feature comparison result;

a password comparator for comparing an input password obtained from the voice of the present user to the generated password to produce a password comparison result; ~~and~~

a controller for determining whether to inhibit the use of the information processing device, depending on the speech feature comparison result and the password comparison result; and

a database storing a plurality of entries, each of which includes address information accompanied with a password check flag,

wherein the information processing device is included in a communication device capable of voice communication, and

wherein, when a telephone dialing request operation occurs, the controller searches the database for address information related to a telephone number corresponding to the telephone dialing request operation and, when the password check flag accompanying the address information found indicates that password check is needed, starts an unauthorized use preventing operation to prevent voice communication to be made to the telephone number corresponding to the telephone dialing request operation.

2. (Original) The unauthorized use prevention apparatus according to claim 1, wherein the generated password is renewed each time the information processing device is put to use.

3. (Original) The unauthorized use prevention apparatus according to claim 1, wherein the password notifying section comprises a display section for displaying the generated password on screen so as to prompt the present user to sound out the generated password.

4. (Original) The unauthorized use prevention apparatus according to claim 1, wherein the password notifying section comprises a speech processor for sounding out the generated password through a speaker so as to prompt the present user to sound out the generated password.

5. (Canceled).

6. (Currently Amended) The unauthorized use prevention apparatus according to claim [[5]] 1, wherein the password generator generates a renewed password in response to a request operation of making a call.

7. (Currently Amended) The unauthorized use prevention apparatus according to claim [[5]] 1, wherein the password generator generates a renewed password in response to a request operation of taking an incoming call.

8. (Currently Amended) The unauthorized use prevention apparatus according to claim [[5]] 1, further comprising:

a database storing a plurality of entries, each of which includes address information accompanied with a password check flag,

wherein, when a request operation occurs, the controller searches the database for address information related to the request operation and, when the password check flag accompanying the address information found indicates that password check is needed, starts an unauthorized use preventing operation.

9. (Currently Amended) A method for preventing unauthorized use of an information processing device, comprising:

a) registering identifying speech feature data previously obtained from voice of an authorized user;

b) generating a password which is a string of arbitrary characters;

c) receiving voice of a present user sounding out the generated password;

d) comparing input speech feature data obtained from the voice of the present user to the identifying speech feature data to produce a speech feature comparison result;

e) comparing an input password obtained from the voice of the present user to the generated password to produce a password comparison result; and

f) determining whether to inhibit the use of the information processing device, depending on the speech feature comparison result and the password comparison result; and

g) storing a plurality of entries corresponding to telephone numbers, each of which includes address information accompanied with a password check flag;

when a telephone call request operation occurs to initiate a telephone call to a destination telephone number, searching the plurality of entries for address information of the destination telephone call related to the telephone call request operation; and

when the password check flag accompanying the address information found indicates that password check is needed, starting the steps b)-f).

10. (Original) The method according to claim 9, wherein the generated password is renewed each time the information processing device is put to use.

11. (Original) The method according to claim 9, wherein the generated password is displayed on a display of the information processing device so as to prompt the present user to sound out the generated password.

12. (Original) The method according to claim 9, wherein the generated password is sounded out through a speaker of the information processing device so as to prompt the present user to sound out the generated password.

13. (Canceled).

14. (Currently Amended) A computer readable medium storing a program, which, when executed by a computer, instructing [[a]] the computer to prevent unauthorized use of an information processing device, comprising:

a) registering identifying speech feature data previously obtained from voice of an authorized user;

b) generating a password which is a string of arbitrary characters;

c) receiving voice of a present user sounding out the generated password;

d) comparing input speech feature data obtained from the voice of the present user to the identifying speech feature data to produce a speech feature comparison result;

e) comparing an input password obtained from the voice of the present user to the generated password to produce a password comparison result; and

f) determining whether to inhibit the use of the information processing device, depending on the speech feature comparison result and the password comparison result; and

g) storing a plurality of entries corresponding to telephone numbers, each of which includes address information accompanied with a password check flag;

when a telephone call request operation occurs to initiate a telephone call to a destination telephone number, searching the plurality of entries for address information of the destination telephone call related to the telephone call request operation; and

when the password check flag accompanying the address information found indicates that password check is needed, starting the steps b)-f).

15. (Currently Amended) The ~~program~~ computer readable medium according to claim 14, wherein the generated password is renewed each time the information processing device is put to use.

16. (Canceled).

17. (New) The unauthorized use prevention apparatus according to claim 1, wherein, when a second telephone dialing request operation occurs, the controller searches the database for address information related to a second telephone number corresponding to the second telephone dialing request operation and, when the password check flag accompanying the address information found indicates that password check is not needed,

allows operation to set up voice communication to be made to the second telephone number corresponding to the second telephone dialing request operation.

18. (New) The method according to claim 9, wherein, when a second telephone dialing request operation occurs, the method comprises:

searching a database for address information related to a second telephone number corresponding to the second telephone dialing request operation and, when the password check flag accompanying the address information found in the database indicates that password check is not needed, allowing operation to set up voice communication to be made to the second telephone number corresponding to the second telephone dialing request operation.

19. (New) The computer readable medium according to claim 14, wherein, when a second telephone dialing request operation occurs, the method comprises:

searching a database for address information related to a second telephone number corresponding to the second telephone dialing request operation and, when the password check flag accompanying the address information found in the database indicates that password check is not needed, allowing operation to set up voice communication to be made to the second telephone number corresponding to the second telephone dialing request operation.